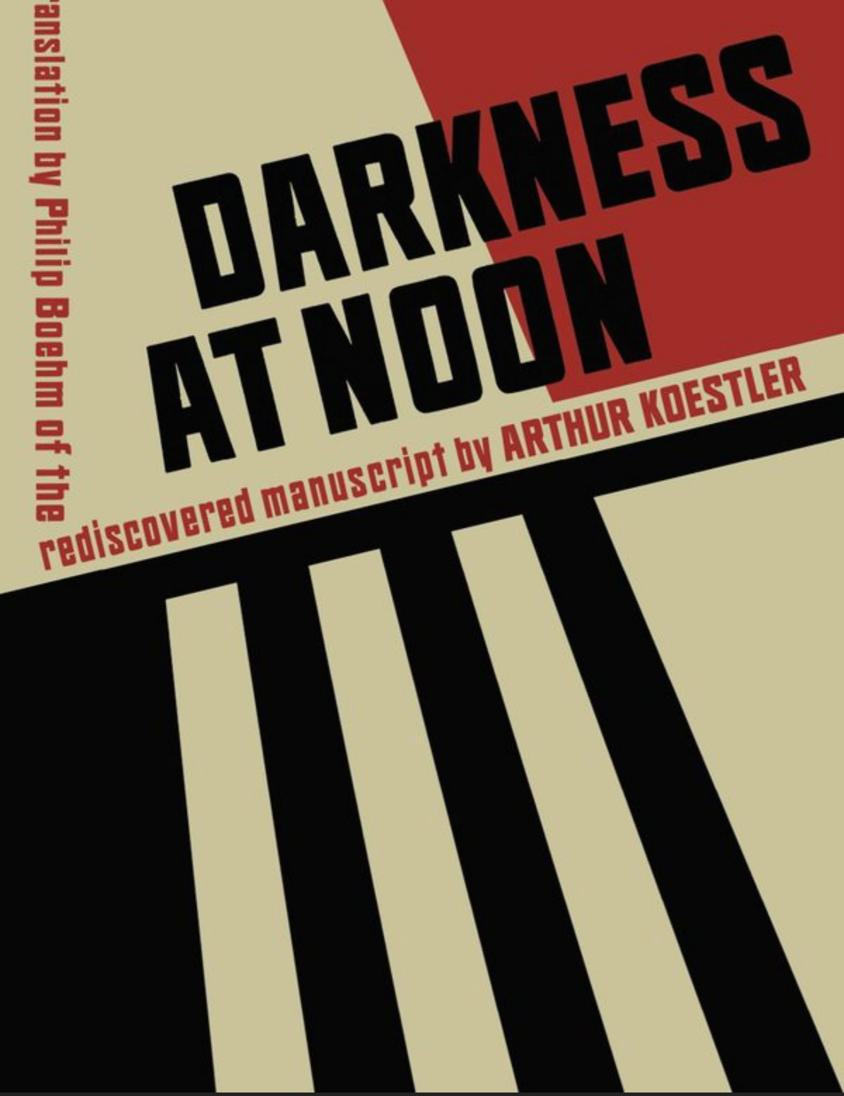
CHINA

Darkness at Noon 01 - WAXTITAN

Why was the National Security Agency targeting Netsential, the major hosting provider for the Department of Homeland Security? Who is behind the IP address 64.9.146.208?

GHOST
2 JUL 2020 • 9 MIN READ



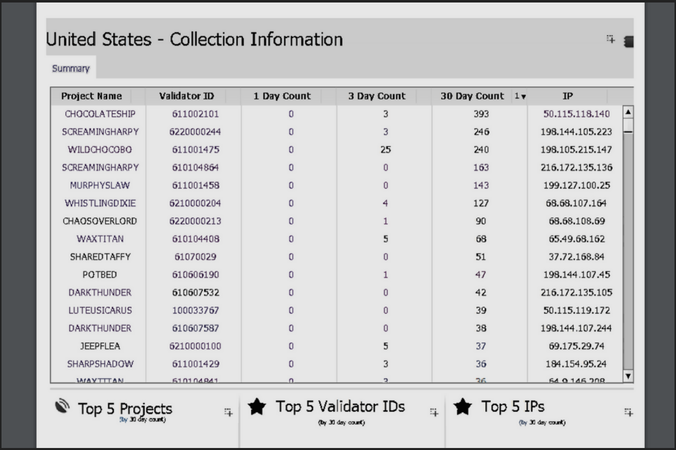
DARKNESS AT NOON

anslation by Phillip Boehm of the rediscovered manuscript by ARTHUR KOESTLER

IP Address #16, WAYTITAN, and the YHC Corporation

As part of the Edward Snowden leaks, a single document was made available that showed the top 16 IP addresses the NSA was targeting in North America.

At the very bottom of the list, address #16, was 64.9.146.208.

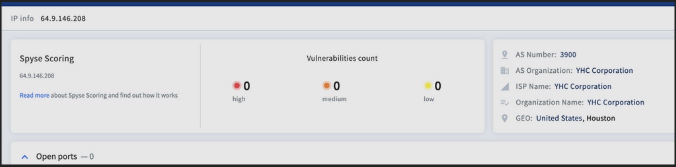


United States - Collection Information

Project Name	Validator ID	1 Day Count	3 Day Count	30 Day Count 1▼	IP
CHOCOLATESHIP	611002101	0	3	393	50.115.118.140
SCREAMINGHARPY	6220000244	0	3	246	198.144.105.223
WILDCHOCOBO	611001475	0	25	240	198.105.215.147
SCREAMINGHARPY	610104864	0	0	163	216.172.135.136
MURPHYSLAW	611001458	0	0	143	199.127.100.25
WHISTLINGDIXIE	6210000204	0	4	127	68.68.107.164
CHAOSOVERLORD	6220000213	0	1	90	68.68.108.69
WAXTITAN	610104408	0	5	68	65.49.68.162
SHAREDTAFFY	61070029	0	0	51	37.72.168.84
POTBED	610606190	0	1	47	198.144.107.45
DARKTHUNDER	610607532	0	0	42	216.172.135.105
LUTEUSICARUS	100033767	0	0	39	50.115.119.172
DARKTHUNDER	610607587	0	0	38	198.144.107.244
JEEPFLEA	6210000100	0	5	37	69.175.29.74
SHARPSHADOW	611001429	0	3	36	184.154.95.24
WAYTITAN	610104841	0	3	36	64.9.146.208

IP address 64.9.146.208 is at the bottom of the list. NSA Codename "WAYTITAN"

This IP address belongs to the same party then as it does now, the mysterious "YHC Corporation". A few things turn up on the internet for the acronym YHC, but nothing that we've seen shows or describes a "YHC Corporation". Except for one place.



IP info 64.9.146.208

Spyse Scoring

64.9.146.208

Read more about Spyse Scoring and find out how it works

Vulnerabilities count

high	medium	low
0	0	0

AS Number: 3900

AS Organization: YHC Corporation

ISP Name: YHC Corporation

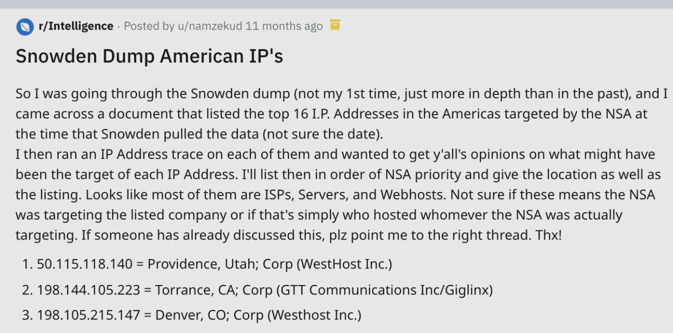
Organization Name: YHC Corporation

GEO: United States, Houston

Open ports — 0

ICANN maintains WHOIS, the database that documents ownership of domain names and IP address blocks. This is the only place "YHC Corporation" seems to turn up, and it is as owner of 64.9.146.208.

I can only find one place on the internet where this was discussed, a single Reddit thread made by a poster who only posted this, and nothing else, 11 months ago.



r/Intelligence · Posted by u/namzekud 11 months ago

Snowden Dump American IP's

So I was going through the Snowden dump (not my 1st time, just more in depth than in the past), and I came across a document that listed the top 16 I.P. Addresses in the Americas targeted by the NSA at the time that Snowden pulled the data (not sure the date).
I then ran an IP Address trace on each of them and wanted to get y'all's opinions on what might have been the target of each IP Address. I'll list then in order of NSA priority and give the location as well as the listing. Looks like most of them are ISPs, Servers, and Webhosts. Not sure if these means the NSA was targeting the listed company or if that's simply who hosted whomever the NSA was actually targeting. If someone has already discussed this, plz point me to the right thread. Thx!

1. 50.115.118.140 = Providence, Utah; Corp (WestHost Inc.)
2. 198.144.105.223 = Torrance, CA; Corp (GTT Communications Inc/Giglinx)
3. 198.105.215.147 = Denver, CO; Corp (Westhost Inc.)

> 4. 216.172.135.136 = San Jose, CA; Corp (EGIHosting)
> 5. 199.127.100.25 = Coquitlam, BC, Canada; Corp (Avesta Networks LLC)
> 6. 68.68.107.164 = San Jose, CA; Corp (EGIHosting)
> 7. 68.68.108.69 = San Jose, CA; Corp (EGIHosting)
> 8. 65.49.68.162 = multi listed addresses: Fremont, CA & Shanghai, China; Corp (Hurricane Electric LLC)
> 9. 37.72.168.84 = multi listed addresses: Chicago, IL & Amsterdam, Netherlands; Corp (Swiftway Sp. z o.o.)
> 10. 198.144.107.45 = Torrance, CA; Corp (Giglinx)
> 11. 216.172.135.105 = San Jose, CA; Corp (EGIHosting/AFNCA)
> 12. 50.115.119.172 = multi listed addresses: Providence, Utah & Newark, NJ; Corp (WestHost Inc.)
> 13. 198.144.107.244 = Torrance, CA; Corp (GTT Communications Inc/Giglinx)
> 14. 69.175.29.74 = multi listed addresses: Chicago, IL & Tempe, AZ; Corp (Singlehop LLC/inap.com)
> 15. 184.154.95.24 = Chicago Loop, IL; Corp (SingleHop LLC)
> 16. 64.9.146.208 = multi listed addressess: Houston, TX & Los Angeles, CA & Roy, Utah & ; Corp(s) (YHC Corp/Insync Internet Services/GFI West/host-line.net)

They also own something else.

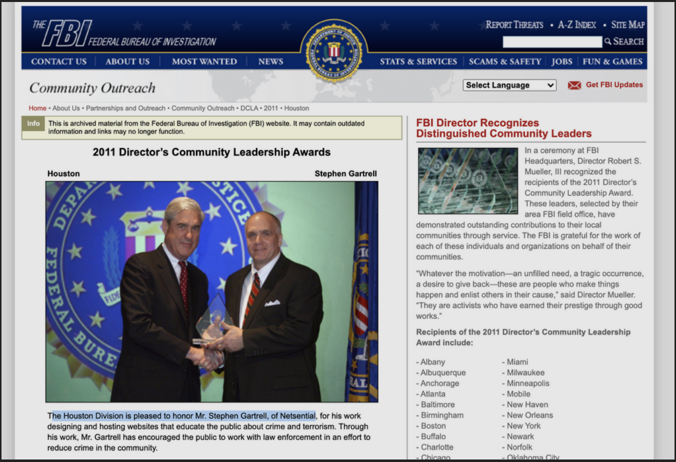
BlueLeaks and Netsential -> YHC Corporation

Several days ago, every DHS Fusion Center, numerous local police agencies, and intelligence sharing groups that report to the DEA were hit in an extremely professional hack followed by document leak.

All of these groups, which was at least 200 different agencies, were hosted by Netsential.com. When we say "hosting" we mean managing the physical servers (think Dell blade computers for instance) that these websites ran on top of. Each website was essentially a

SaaS application for each agency. You would sign in, get intelligence, upload data, etc. Because the source code was dumped, we also know that Netsential developed the very applications themselves.

The below result shows an interesting award from former FBI director Robert Mueller to Stephen Gartrell of Netsential. One of the few records available of this company anywhere. This result appears to be deindexed by Google interestingly, and was only sent to us by another researcher.


THE FBI FEDERAL BUREAU OF INVESTIGATION
REPORT THREATS • A-Z INDEX • SITE MAP
SEARCH
CONTACT US | ABOUT US | MOST WANTED | NEWS
STATS & SERVICES | SCAMS & SAFETY | JOBS | FUN & GAMES
Select Language
Get FBI Updates

Community Outreach

Home • About Us • Partnerships and Outreach • Community Outreach • DCLA • 2011 • Houston

Info This is archived material from the Federal Bureau of Investigation (FBI) website. It may contain outdated information and links may no longer function.

2011 Director's Community Leadership Awards

Houston **Stephen Gartrell**

The Houston Division is pleased to honor Mr. Stephen Gartrell, of Netsential, for his work designing and hosting websites that educate the public about crime and terrorism. Through his work, Mr. Gartrell has encouraged the public to work with law enforcement in an effort to reduce crime in the community.

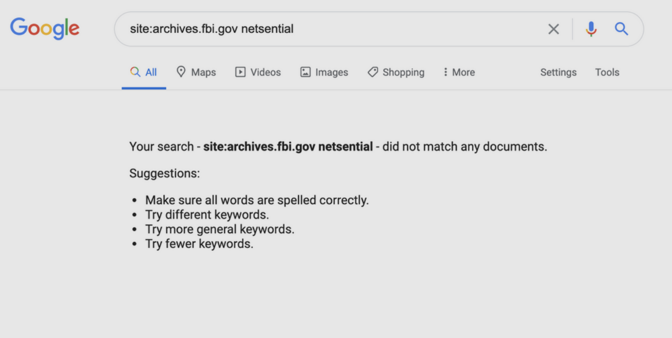
FBI Director Recognizes Distinguished Community Leaders

In a ceremony at FBI Headquarters, Director Robert S. Mueller, III recognized the recipients of the 2011 Director's Community Leadership Award. These leaders, selected by their area FBI field office, have demonstrated outstanding contributions to their local communities through service. The FBI is grateful for the work of each of these individuals and organizations on behalf of their communities.

"Whatever the motivation—an unfilled need, a tragic occurrence, a desire to give back—these are people who make things happen and enlist others in their cause," said Director Mueller. "They are activists who have earned their prestige through good works."

Recipients of the 2011 Director's Community Leadership Award include:

- Albany
- Albuquerque
- Anchorage
- Atlanta
- Baltimore
- Birmingham
- Boston
- Buffalo
- Charlotte
- Chicago
- Miami
- Milwaukee
- Minneapolis
- Mobile
- New Haven
- New Orleans
- New York
- Newark
- Norfolk
- Oklahoma City



site:archives.fbi.gov netsential

Your search - **site:archives.fbi.gov netsential** - did not match any documents.

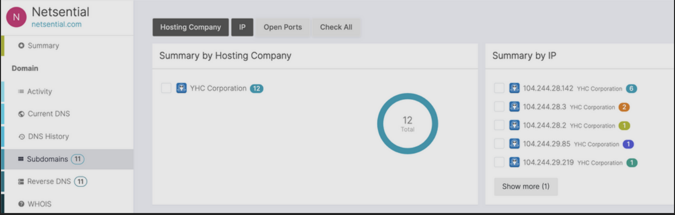
Suggestions:

- Make sure all words are spelled correctly.
- Try different keywords.
- Try more general keywords.
- Try fewer keywords.

Netsential seem to do quite a bit, developing software and managing data center servers isn't an easy business.

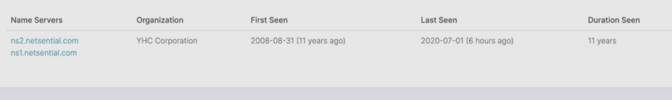
Things get very concerning though when we look at Passive DNS records and WHOIS data for Netsential. Below is a screenshot from the wonderful service, SecurityTrails.com, that brilliantly aggregates this - and more services like Certificate Transparency logs - in a single dashboard.

Had we been able to use Farsight Security this week, I'm sure the data would have been even better. Another post will follow with data from that company, whose founder helped co-invent the DNS over three decades ago.



104.244.28.142 YHC Corporation 6
104.244.28.3 YHC Corporation 2
104.244.28.2 YHC Corporation 1
104.244.29.85 YHC Corporation 1
104.244.29.219 YHC Corporation 1

Also by extracting all of the domain names from the various name servers Netsential ran (ns1.netsential.com and ns2.netsential.com) it seems their *only* customers were government law enforcement agencies across local, state, and federal groups. The full list can be viewed below or at this link.



Name Servers	Organization	First Seen	Last Seen	Duration Seen
ns2.netsential.com ns1.netsential.com	YHC Corporation	2008-08-31 (11 years ago)	2020-07-01 (6 hours ago)	11 years

The two Netsential name servers from which all websites they hosted were extracted. This screenshot also shows their ownership by the "YHC Corporation". Netsential was first recorded August of 2008, but could have existed before.

They in turn we can see were part of, according to WHOIS data they would have filed and on record with ICANN, the YHC Corporation.

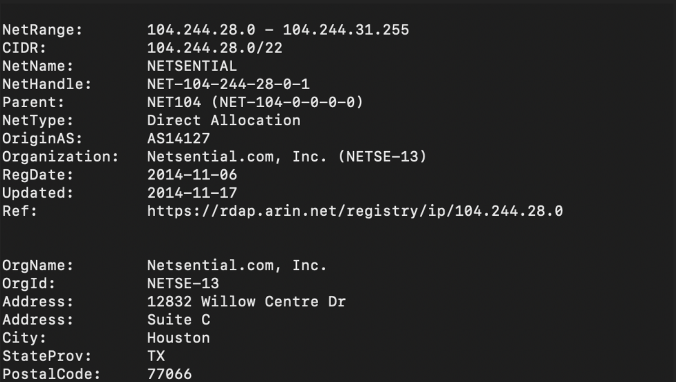
So in addition to having what looks like one owner

(YHC), they also have what looks like a single customer, law enforcement intelligence groups/fusion centers. And Netsential has almost as little about it on the internet as YHC. What is going on here?

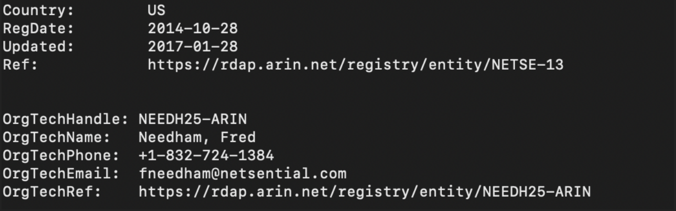
A 2013 Hack That Came From Netsential Servers

As a quick aside, this isn't the first time Netsential has been implicated in malicious events.

The IP address of 104.244.30.220, part of a whole /22 block Netsential owns, was implicated in several hacks - after the Snowden leak as well we should mention. So this wasn't the original reason the NSA targeted them.

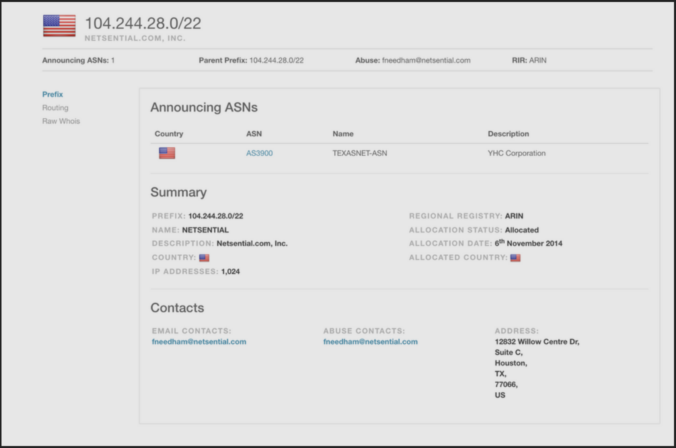


```
NetRange:       104.244.28.0 - 104.244.31.255
CIDR:           104.244.28.0/22
NetName:        NETSENTIAL
NetHandle:      NET-104-244-28-0-1
Parent:         NET104 (NET-104-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS14127
Organization:   Netsential.com, Inc. (NETSE-13)
RegDate:        2014-11-06
Updated:        2014-11-17
Ref:            https://rdap.arin.net/registry/ip/104.244.28.0


OrgName:        Netsential.com, Inc.
OrgId:          NETSE-13
Address:        12832 Willow Centre Dr
Address:        Suite C
City:           Houston
StateProv:      TX
PostalCode:     77066
```



```
Country:        US
RegDate:        2014-10-28
Updated:        2017-01-28
Ref:            https://rdap.arin.net/registry/entity/NETSE-13


OrgTechHandle: NEEDH25-ARIN
OrgTechName:   Needham, Fred
OrgTechPhone:  +1-832-724-1384
OrgTechEmail:  fneedham@netsential.com
OrgTechRef:    https://rdap.arin.net/registry/entity/NEEDH25-ARIN
```

A manual whois query made from the Terminal showing Netsential ownership of the 104.244.28.0/22 block.



104.244.28.0/22
NETSENTIAL.COM, INC.

Announcing ASNs: 1 **Parent Prefix:** 104.244.28.0/22 **Abuse:** fneedham@netsential.com **RIR:** ARIN

Announcing ASNs

Country	ASN	Name	Description
🇺🇸	AS3900	TEXASNET-ASN	YHC Corporation

Summary

PREFIX: **104.244.28.0/22**
NAME: **NETSENTIAL**
DESCRIPTION: **Netsential.com, Inc.**
COUNTRY: 🇺🇸
IP ADDRESSES: **1,024**
REGIONAL REGISTRY: **ARIN**
ALLOCATION STATUS: **Allocated**
ALLOCATION DATE: **6th November 2014**
ALLOCATED COUNTRY: 🇺🇸

Contacts

EMAIL CONTACTS: fneedham@netsential.com
ABUSE CONTACTS: fneedham@netsential.com
ADDRESS:
12832 Willow Centre Dr,
Suite C,
Houston,
TX,
77066,
US

A screenshot from the service BGPview.io

This is partly documented here on an Otava blog post titled "Recommendations To Combat CryptoLocker Malware". Netsential's name turns up, along with the National Fusion Center Association.

Spoofed Sender: “fraud@aexp.com” “Dewayne@nfcausa.org”
Sender IP: 209.143.144.3
Sender Host: mail.netsential.com

Netsential was a Fraud Meant to Conceal Illegal Actions

First, Netsential is a front company **meant to hide** law enforcement data, but particularly Department of Homeland Security data, **from legislative bodies and American citizens**.

That is the only reason they would have made to forgo vastly cheaper options with dozens of more features like AWS, Azure, or even the San Antonio, Texas based Rackspace. Any reason they would have would be deception based.

I should also mention at this point that **it was illegal to host data at most points in the last decade with Netsential because of something known as "CJIS"**. More on this later though.

Again, all the **classic signs of fraud are there**. Obvious different companies that could have been chosen that would have been much better solutions, less expensive, and definitely more clearly lawful. A single major customer. A single owner that in turn likely has another owner (a chain of shell companies essentially). And so on.

Anytime DHS has been asked to hand over records, they don't hand over Netsential records. And they never will. The fact that a certain government agency has hidden (via robots.txt) an award presented to the owner of Netsential in 2011 by a major figure in the Justice Department is not a good sign. We will post this later.

We're not going to write a 90 page Department of Justice indictment here on the fraud angle. And when we say fraud, we mean more that it is defrauding others out of political power. Some form of financial deception is certainly here, but do not get distracted by it. It is a kind of fraud nonetheless, and the forensic evidence we leave to others. Finally we aren't going to waste time to entertain opinions that think these risks and sacrifices would have been made by those with good intentions. We hate to be this direct and aggressive with our language, but you would be either a fool or a shill, and certainly not a good engineer, to think this.

Netsential Was Illegally Hosting Data Because of CJIS:

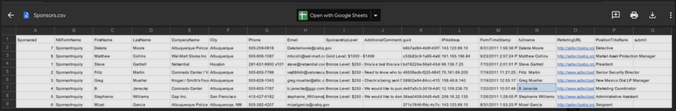
First, we know a lot about CJIS, having directly managed thousands of servers for the Department of Information Resources in Texas. DIR provides IT for all 37 State of Texas agencies, and about 40% of all machines. This includes working with AWS Gov Cloud, Azure Gov Cloud, and the now Atos-managed data centers in Austin and San Angelo.

In fact one of our founders, Dan Ehrlich, lives less than a mile from the only CJIS-compliant data center in all of Texas, Azure South.

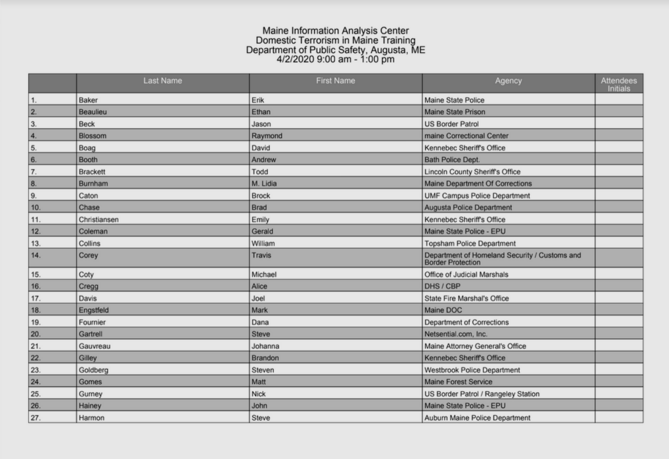
This section we will update later to document in excruciating detail why they were not in CJIS compliance, which is a very big deal. Part of the reason Azure South was to be a CJIS compliant cloud - the very first in fact - and to have it in Texas, a state with a very large prison population.

One part of CJIS compliance they did have though. Logging of all IPs that ever accessed their data, stored in detail in CSV and Microsoft Word files. We will leave to others to make fun of this quite awful engineering decision, and we will grant that maybe this was done as an attempt to be "sort of" in CJIS compliance, which requires audit trails, at one time.

Of course these same logs now could also be used as evidence against Netsential to show a wide array of *successful* hacking attempts from across the world, consistent access from different government agencies, and exfiltration of all of their data - repeatedly - to a major foreign power the US stands in opposition to. This data will be analyzed in either a third of fourth post in this series. Some screenshots below have been posted as brief proof of their extensiveness and detail. We want to emphasize our deep respect for law enforcement, many of whom have served or co-serve in the military. They can write us at zephyrus@12security.com and we will respond to any at least partially reasonable sounding takedown requests within the hour.

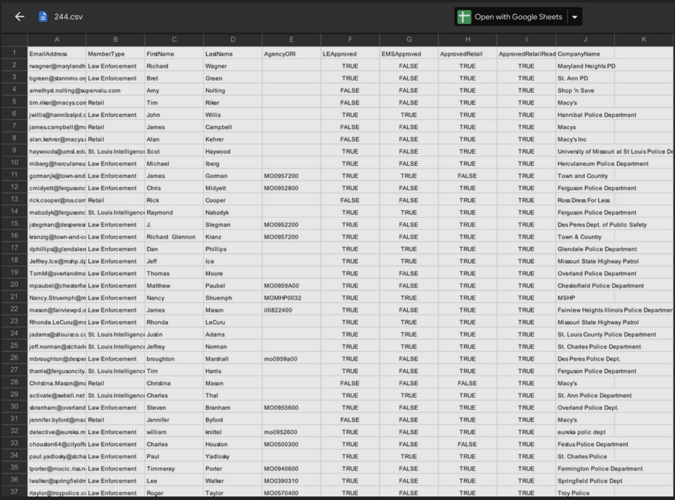


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Sponsorid	NSFormName	FirstName	LastName	CompanyName	City	Phone	Email	SponsorshipLevel	AdditionalComments	guid	IPAddress	FormTimeStamp	fullname	ReferringURL	PositionTitleRank	submit
2	7	SponsorInquiry	Dakota	Moore	Albuquerque Police	Albuquerque	505-259-0816	Dakotamoore@cabq.gov			b6b7ad94-4b9f-43f7	143.120.99.10	8/31/2011 1:56:36 P	Dakota Moore	http://safecityabq.or	Detective	
3	8	SponsorInquiry	Matthew	Collins	Wal-Mart Stores Inc	Albuquerque	505-906-1087	mbcolli@wal-mart.c	Gold Level: $1000 - $1499		c53b83c9-1a95-4a9	161.165.196.84	9/23/2011 2:57:24 P	Matthew Collins	http://safecityabq.or	Market Asset Protection Manager	
4	1	SponsorInquiry	Steve	Gartrell	Netsential	Houston	281-631-9900 x101	steve@netsential.co	Bronze Level: $250 -	this is a test this is a t	bd16224a-56a0-43d	66.136.7.25	7/15/2011 2:01:01 P	Steve Gartrell	http://safecityabq.or	President	
5	2	SponsorInquiry	Fritz	Martin	Coronado Center / V	Albuquerque	505-855-7786	vsa584dir@valorsecu	Bronze Level: $250 -	Need to know who to	46506edb-f225-4845	75.161.69.205	7/19/2011 11:21:25	Fritz Martin	http://www.safecityat	Senior Security Director	
6	3	SponsorInquiry	Greg	Mueller	Kroger / Smith's Foo	Albuquerque	505-828-1043	greg.mueller@sfdc.c	Bronze Level: $250 -	Check is being sent f	58902e94-84cc-415	158.48.6.140	7/19/2011 12:55:17	Greg Mueller	http://www.safecityat	New Mexico Dist LP Manager	
7	4	SponsorInquiry	B	Janecka	Coronado Center	Albuquerque	505-855-7787	b.janecka@ggp.com	Bronze Level: $250 -	We would like to pur	de97a5c5-3019-4d0	12.109.236.75	7/20/2011 10:57:49	B Janecka	http://www.safecityat	Marketing Coordinator	
8	5	SponsorInquiry	Stephanie	Williams	Gap Inc.	San Francisco	415-427-0182	stephanie_Williams	Bronze Level: $250 -	We would like to don	36aa0458-04d5-4e5	206.16.32.135	7/26/2011 1:28:05 P	Stephanie Williams	http://www.safecityat	Administrative Assistant	
9	6	SponsorInquiry	Mizel	Garcia	Albuquerque Police	Albuqueruqe, NM	505-382-4207	mizelgarcia@cabq.gov			371c7646-ffdc-4c7c	143.120.99.10	8/31/2011 1:53:25 P	Mizel Garcia	http://safecityabq.or	Sergeant	



Maine Information Analysis Center
Domestic Terrorism in Maine Training
Department of Public Safety, Augusta, ME
4/2/2020 9:00 am - 1:00 pm

	Last Name	First Name	Agency	Attendees Initials
1.	Baker	Erik	Maine State Police	
2.	Beaulieu	Ethan	Maine State Prison	
3.	Beck	Jason	US Border Patrol	
4.	Blossom	Raymond	maine Correctional Center	
5.	Boag	David	Kennebec Sheriff's Office	
6.	Booth	Andrew	Bath Police Dept.	
7.	Brackett	Todd	Lincoln County Sheriff's Office	
8.	Burnham	M. Lidia	Maine Department Of Corrections	
9.	Caton	Brock	UMF Campus Police Department	
10.	Chase	Brad	Augusta Police Department	
11.	Christiansen	Emily	Kennebec Sheriff's Office	
12.	Coleman	Gerald	Maine State Police - EPU	
13.	Collins	William	Topsham Police Department	
14.	Corey	Travis	Department of Homeland Security / Customs and Border Protection	
15.	Coty	Michael	Office of Judicial Marshals	
16.	Cregg	Alice	DHS / CBP	
17.	Davis	Joel	State Fire Marshal's Office	
18.	Engstfeld	Mark	Maine DOC	
19.	Fournier	Dana	Department of Corrections	
20.	Gartrell	Steve	Netsential.com, Inc.	
21.	Gauvreau	Johanna	Maine Attorney General's Office	
22.	Gilley	Brandon	Kennebec Sheriff's Office	
23.	Goldberg	Steven	Westbrook Police Department	
24.	Gomes	Matt	Maine Forest Service	
25.	Gurney	Nick	US Border Patrol / Rangeley Station	
26.	Hainey	John	Maine State Police - EPU	
27.	Harmon	Steve	Auburn Maine Police Department	

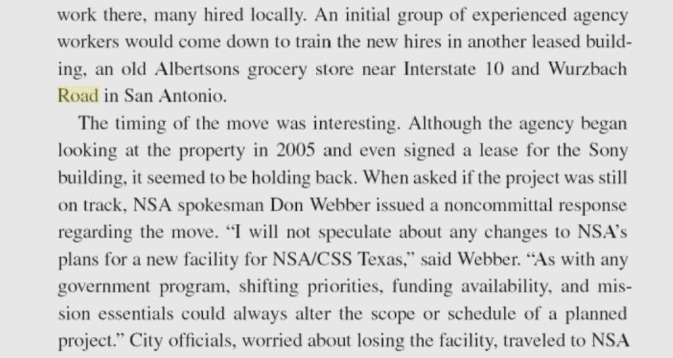


	A	B	C	D	E	F	G	H	I	J	K
1	EmailAddress	MemberType	FirstName	LastName	AgencyORI	LEApproved	EMSApproved	ApprovedRetail	ApprovedRetailRead	CompanyName	
2	rwagner@marylandh	Law Enforcement	Richard	Wagner		TRUE	FALSE	TRUE	TRUE	Maryland Heights PD	
3	bgreen@stannmo.or	Law Enforcement	Bret	Green		TRUE	FALSE	TRUE	TRUE	St. Ann PD	
4	amethyst.nolting@supervalu.com		Amy	Nolting		FALSE	FALSE	TRUE	TRUE	Shop 'n Save	
5	tim.riker@macys.con	Retail	Tim	Riker		FALSE	FALSE	TRUE	TRUE	Macy's	
6	jwillis@hannibalpd.c	Law Enforcement	John	Willis		TRUE	TRUE	TRUE	TRUE	Hannibal Police Department	
7	james.campbell@ma	Retail	James	Campbell		FALSE	FALSE	TRUE	TRUE	Macys	
8	alan.kehrer@macys.c	Retail	Alan	Kehrer		FALSE	FALSE	TRUE	TRUE	Macy's Inc	
9	haywoods@umsl.edu	St. Louis Intelligence	Scot	Haywood		TRUE	FALSE	TRUE	TRUE	University of Missouri at St Louis Police De	
10	miberg@herculaneu	Law Enforcement	Michael	Iberg		TRUE	FALSE	TRUE	TRUE	Herculaneum Police Department	
11	gormanjk@town-and-	Law Enforcement	James	Gorman	MO0957200	TRUE	TRUE	FALSE	TRUE	Town and Country	
12	cmidyett@fergusonc	Law Enforcement	Chris	Midyett	MO0952800	TRUE	FALSE	TRUE	TRUE	Ferguson Police Department	
13	rick.cooper@ros.com	Retail	Rick	Cooper		FALSE	FALSE	TRUE	TRUE	Ross Dress For Less	
14	mabzdyk@fergusonc	St. Louis Intelligence	Raymond	Nabzdyk		TRUE	TRUE	TRUE	TRUE	Ferguson Police Department	
15	jstegman@desperes	Law Enforcement	J.	Stegman	MO0952200	TRUE	FALSE	TRUE	TRUE	Des Peres Dept. of Public Safety	
16	kranzrg@town-and-c	Law Enforcement	Richard Glennon	Kranz	MO0957200	TRUE	FALSE	TRUE	TRUE	Town & Country	
17	dphillips@glendalen	Law Enforcement	Dan	Phillips		TRUE	TRUE	TRUE	TRUE	Glendale Police Department	
18	Jeffrey.Ice@mshp.dp	Law Enforcement	Jeff	Ice		TRUE	TRUE	TRUE	TRUE	Missouri State Highway Patrol	
19	TomM@overlandmo	Law Enforcement	Thomas	Moore		TRUE	FALSE	TRUE	TRUE	Overland Police Department	
20	mpaubel@chesterfie	Law Enforcement	Matthew	Paubel	MO0959A00	TRUE	FALSE	TRUE	TRUE	Chesterfield Police Department	
21	Nancy.Struemph@m	Law Enforcement	Nancy	Struemph	MOMHP0032	TRUE	TRUE	TRUE	TRUE	MSHP	
22	mason@fairviewpd.o	Law Enforcement	James	Mason	il0822400	TRUE	FALSE	TRUE	TRUE	Fairview Heights Illinois Police Departmer	
23	Rhonda.LeCuru@ms	Law Enforcement	Rhonda	LeCuru		TRUE	TRUE	TRUE	TRUE	Missouri State Highway Patrol	
24	jadams@stlouisco.cc	St. Louis Intelligence	Justin	Adams		TRUE	TRUE	TRUE	TRUE	St. Louis County Police Department	
25	jeff.norman@stcharl	St. Louis Intelligence	Jeffrey	Norman		TRUE	TRUE	TRUE	TRUE	St. Charles Police Department	
26	mbroughton@desper	Law Enforcement	broughton	Marshall	mo0959a00	TRUE	FALSE	TRUE	TRUE	Des Peres Police Dept.	
27	tharris@fergusoncity.	St. Louis Intelligence	Tim	Harris		TRUE	FALSE	TRUE	TRUE	Ferguson Police Department	
28	Christina.Mason@ma	Retail	Christina	Mason		FALSE	FALSE	FALSE	TRUE	Macy's	
29	activate@swbell.net	St. Louis Intelligence	Charles	Thal		TRUE	TRUE	TRUE	TRUE	St. Ann Police Department	
30	sbranham@overland	Law Enforcement	Steven	Branham	MO0955600	TRUE	FALSE	TRUE	TRUE	Overland Police Dept.	
31	jennifer.byford@mac	Retail	Jennifer	Byford		FALSE	FALSE	TRUE	TRUE	Macy's	
32	detective@eureka.m	Law Enforcement	william	knittel	mo0952600	TRUE	FALSE	TRUE	TRUE	eureka polic dept	
33	chouston64@cityoffe	Law Enforcement	Charles	Houston	MO0500300	TRUE	FALSE	FALSE	TRUE	Festus Police Department	
34	paul.yadlosky@stcha	Law Enforcement	Paul	Yadlosky		TRUE	TRUE	TRUE	TRUE	St. Charles Police	
35	tporter@mocic.riss.n	Law Enforcement	Timmeray	Porter	MO0940600	TRUE	FALSE	TRUE	TRUE	Farmington Police Department	
36	lwalker@springfieldm	Law Enforcement	Lee	Walker	MO0390310	TRUE	FALSE	TRUE	TRUE	Springfield Police Dept	
37	rtaylor@troypolice.cc	Law Enforcement	Roger	Taylor	MO0570400	TRUE	FALSE	TRUE	TRUE	Troy Police	

The NSA Datacenter Right By Netsential

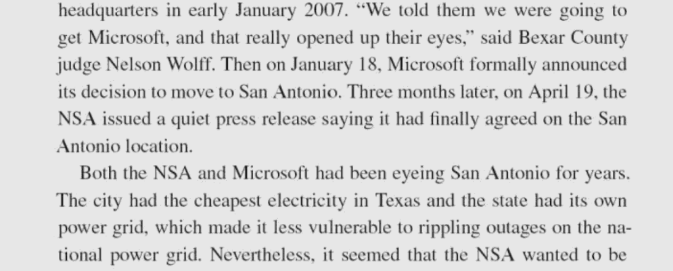
The fact that the NSA was so heavily targeting Netsential is very curious to us.

Azure South, a far better option where all this data could have been hosted, is of course also known as "NSA South". It is the 5150 Roger's Road, San Antonio, Texas Data Center. Since the NSA realized in the early 2000's how devastating an attack on the power grid would be, they have built data centers across the country that help to process their massive data stores along with providing alternative electricity sites. Texas has not only a separate electrical grid from all other states, it has some of the lowest electricity costs in the nation. When breaking an 2048-bit RSA key can cost (at one time) something like $1,000 a break, these costs add up quickly.



work there, many hired locally. An initial group of experienced agency workers would come down to train the new hires in another leased building, an old Albertsons grocery store near Interstate 10 and Wurzbach Road in San Antonio.

The timing of the move was interesting. Although the agency began looking at the property in 2005 and even signed a lease for the Sony building, it seemed to be holding back. When asked if the project was still on track, NSA spokesman Don Webber issued a noncommittal response regarding the move. "I will not speculate about any changes to NSA's plans for a new facility for NSA/CSS Texas," said Webber. "As with any government program, shifting priorities, funding availability, and mission essentials could always alter the scope or schedule of a planned project." City officials, worried about losing the facility, traveled to NSA



headquarters in early January 2007. "We told them we were going to get Microsoft, and that really opened up their eyes," said Bexar County judge Nelson Wolff. Then on January 18, Microsoft formally announced its decision to move to San Antonio. Three months later, on April 19, the NSA issued a quiet press release saying it had finally agreed on the San Antonio location.

Both the NSA and Microsoft had been eyeing San Antonio for years. The city had the cheapest electricity in Texas and the state had its own power grid, which made it less vulnerable to rippling outages on the national power grid. Nevertheless, it seemed that the NSA wanted to be

A screenshot from James Bamford's book "The Shadow Factory"

The 5150 Roger's Road Data Center. Also known as "NSA South"

What is most interesting to us however is that Netsential comes online seemingly right around when the data center is first confirmed in the news. The first A record from the DNS we could pull is August 2008 for Netsential. A little over 18 months after the official announcement from the City of San Antonio and only about 6 months from when shovel first hit the dirt in Central Texas.

Two more asides. Back then in 2008 their main IP address for Netsential.com was in the 209.0.0.0/8 space. This is very curious for a reason that a later blog post will get into. As a hint though it has something to do with the National 911 system as well as government SaaS providers like Granicus, GovDelivery, and Gov-I. That single /8 block is among the most contested on the internet, and has been for some time.

We should also note that where they host now, in 104.0.0.0/8, has long been associated with organized crime due to the large sections of it that Cloudflare owns. We'll just note that and move on.

Conclusion

- Netsential was the victim of a major hack and subsequent documents release last week. These documents can be viewed partially here: blueleaks.io
- Netsential is a company in Houston that

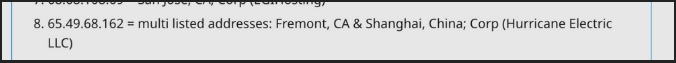
developed applications and hosted them on the internet for hundreds of DHS, Law Enforcement, Department of Justice, and DEA intelligence sites.

- The lack of history of behind this provider and the lack of CJIS compliance (which now jeopardizes perhaps tens of thousands of criminal cases) strongly suggest fraud.
- That Netsential and their equally mysterious owner, YHC Corporation, were one of the top NSA targets in North America at the time of the Edgar Snowden leak is extremely damning. Their extensive IP records, which they kept commingled with police data, now suggest broad hacking from a variety of major nation states nearly continuously for the last few years.

Next Time

- The Chinese Communist Party and their connection to CalCop.org, Fishtech.group, BlueLeaks, and BellTrox - WAYTITAN. Hint: look at the final screenshot
- The extensive hacking of the .gov TLD over

the last 18 months along with .gov.au and Microsoft.



8. 65.49.68.162 = multi listed addresses: Fremont, CA & Shanghai, China; Corp (Hurricane Electric LLC)

MORE IN **CHINA**

Darkness at Noon 02 - WAYTITAN
2 Jul 2020 – 9 min read

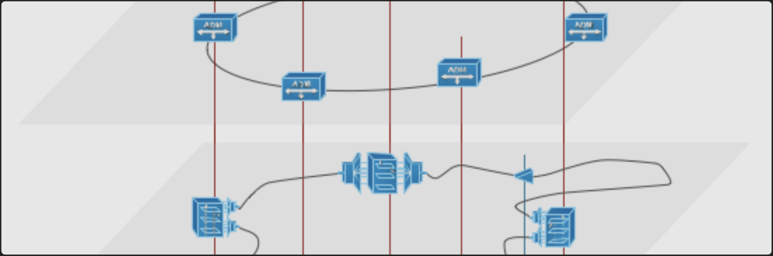
1 post →

CHINA

Darkness at Noon 02 - WAYTITAN

China, the Chinese Communist Party, the history of the internet since 1984, and it's connection to Xinjiang.

DAN EHRLICH
2 JUL 2020 • 9 MIN READ



ENERGY DEPARTMENT

The Overlay Network

And analysis of a malicious botnet based in the DNS that targets government infrastructure.

DAN EHRLICH
30 JUN 2020 • 3 MIN READ